

**Amendments to the Specification:**

Please revise paragraph [0017] as follows:

According to the present invention, the solution to the technical problem posed above is that there are defined both a secret convention of  $p$  key symbols  $K_1, \dots, K_p$  selected from a second alphabet  $B$ , and a multivariate function  $M$  having  $m+1$  variables ( $m \leq N$ ):  $M(X_{i1}, \dots, X_{im}, Y)$  operating  $A^m \times B$  in  $A$ ,  $\{i_1, \dots, i_m\}$  being  $m$  distinct indices in the range  $[1, N]$  and the function  $M$  being ~~objective~~ bijective relative to at least one  $(X_{i1})$  of the  $m$  variables of  $A$ . The enciphering method performs a succession of  $X$  permutations on the sequences  $\{S_1, S_2, \dots, S_N\}$  such that where  $\{S_1, S_2, \dots, S_N\}$  is the sequence prior to the  $j^{\text{th}}$  permutation, the sequence after the  $j^{\text{th}}$  permutation is  $\{S_2, S_3, \dots, S_N, Z_j\}$ , where  $Z_j$  is equal to  $M(S_{i1}, \dots, S_{im}, K_j)$  the enciphered information being constituted by the sequence  $\{S'_1, S'_2, \dots, S'_N\}$  obtained after the  $X^{\text{th}}$  permutation.